CLAIMS

1. A method of manufacturing a series of integrated circuits having related functionality, the method including the steps of:

(a) determining an identifier;

(b) permanently storing the identifier on one of the integrated circuits;

(c) repeating steps (a) and (b) for each integrated circuit in the series;

wherein the identifiers for the series are determined in such a way that knowing the identifier of one of the integrated circuits does not improve the ability of an attacker to determine the identifier of any of the other integrated circuits.

2. A method according to claim 1, wherein the identifier for each integrated circuit is determined using a stochastic mechanism, thereby rendering highly improbable the replication of some or all of the series of identifiers stored on the series of the integrated circuits.

3. A series of integrated circuits having related functionality, wherein each of the integrated circuits incorporates an identifier determined and stored in accordance with claim 1.

4. A series of integrated circuits according to claim 4, wherein each of the integrated circuits is a printer controller.

5. A first integrated circuit of a series of integrated circuits according to claim 3, operable in first and second mode, wherein in the first mode, supervisor code can access the identifier and in the second mode, user code cannot access the identifier.

6. A first integrated circuit according to claim 5, wherein the supervisor mode is available to a program upon verification of that program by a boot program of the integrated circuit.

7. A first integrated circuit according to claim 3, wherein the identifier is mapped into a key K.

8. A first integrated circuit according to claim 7, wherein K is the identifier.

9. A first integrated circuit according to claim 7, wherein K is created by applying a hash function or one-way function to the identifier.

10. A first integrated circuit according to claim 7, configured to produce and output a message from the integrated circuit, the message including a result of encrypting K.

11. A method of injecting a key into a target integrated circuit, comprising the step of receiving the message generated by the first integrated circuit of claim 10, and transferring a second key into the target integrated circuit, the second key being based on K.

12. A method according to claim 11, including generating the second key by:
manipulating K with a function.

13. A method according to claim 12, wherein the function uses K and a code associated with the target integrated circuit as operands.

14. A method according to claim 13, wherein the code is a code that is relatively unique to the target integrated circuit.

15. A method according to claim 14, wherein K and the second key enable secure communication between the first integrated circuit and the target integrated circuit.

16. A method according to claim 15, wherein the second integrated circuit is configured to communicate securely with a third integrated circuit, thereby enabling it to act as an intermediary between the first integrated circuit and the third integrated circuit, allowing secure communication therebetween.

17. A method according to claim 15, wherein the first integrated circuit and the third integrated circuit do not share a key for use in the secure communication.

18. A method according to claim 16, wherein the first integrated circuit is a printer controller configured to perform an authenticated read of the third integrated circuit by securely communicating via the second integrated circuit.

20. A method according to claim 19, wherein the authenticated read relates to monitoring or updating usage of a resource.